WHAT IS CLAIMED IS:

1. In a cable system, an encryption renewal system for generating one or more entitlement control messages, the messages containing cryptographic keys for allowing a subscriber set-top box to decrypt content encrypted off-line, the entitlement control message being forwarded with the content to the subscriber terminal, the encryption renewal system comprising:

a first computing platform for receiving a request to generate the entitlement control messages, the first computing platform performing non-secure tasks associated with the entitlement control messages;

a second computing platform physically separate from the first computing platform for generating the entitlement control messages, the second computing platform performing secure tasks associated with the entitlement control messages; and

one or more firewalls between the first and the second computing platforms for enhancing security of the encryption renewal system, the first computing platform forwarding the entitlement control messages to enable the subscriber set-top box to de-crypt the pre-encrypted content.

2. The system of claim 1 wherein the second computing platform further comprises an application specific integrated circuit chip for generating the entitlement control messages.

3. An encryption renewal system comprising:

a first computing platform for performing non-secure tasks associated with one or more control messages that transmit one or more keys to a subscriber; and

a second computing platform physically separate from the first computing platform containing one or more application specific integrated circuit chip for generating the one or more control messages.

4. The system of claim 3 further comprising one or more firewalls between the first and the second computing platforms.

5. The system of claim 3 further comprising a database for storing the keys to be included in the control messages.

6. The system of claim 3 wherein the key is a group or periodical key from a conditional access system for controlling a population of set-top boxes.

7. The system of claim 3 further comprising a third computing platform physically separate from the first computing platform for performing secure tasks associated with the control messages.

8. The system of claim 7 wherein each of the second and third computing platforms are detachably coupled to the first computing platform.

9. The system of claim 3 wherein the second computing platform further comprises a web server accepting requests from the first computing platform to generate the control messages.

10. The system of claim 7 wherein the second and third computing platforms are initially configured to be identical.

11. The system of claim 3 wherein the second and third computing platforms are interchangeable.

12. The system of claim 3 wherein the control message is generated using the cryptographic key and an encryption record.

13. An encryption renewal system, comprising:

means for receiving an entitlement management message containing one or more cryptographic keys which allows a subscriber of a point to point communication system to access pre-encrypted content;

means for extracting the cryptographic key from the entitlement management message, said means for extracting being physically separate from the means for receiving; and

means for storing the one or more cryptographic keys, said means for receiving and means for extracting performing non-secure and secure processing, respectively, of tasks associated with extracting the one or more cryptographic keys.

14. The system of claim 13 wherein the means for extracting further comprises an application specific integrated for extracting the one or more cryptographic keys.

15. The system of claim 14 wherein the application specific integrated circuit re-encrypts the one or more cryptographic keys for external storage.

16. The system of claim 13 wherein the means for storing stores information about which video on demand system associated with the conditional access system.

17. A method of registering an off-line encryption device in order to begin encrypting clear content, the method using a remotely located encryption renewal system, the method comprising:

generating registration data for registering the off-line encryption device;

encrypting the registration data with one or more cryptographic keys to form encrypted registration data;

forwarding the encrypted registration data to the off-line encryption device; and

retrieving, by the off-line encryption device, the registration data from the encrypted registration data, wherein the off-line encryption device begins to encrypt the clear content intended for and only after the registration data is retrieved.

18. The method of claim 17 further comprising storing the one or more cryptographic keys prior to generating data.

19. The method of claim 17 wherein the data contains both cryptographic keys and one or more operating parameters for the off-line encryption device.

20. The method of claim 19 wherein the operating parameter is a maximum number of encryption sessions allocated to the off-line encryption device.

21. The method of claim 17 where the step of generating further comprises determining the operating parameters of the off-line encryption device.

22. The method of claim 18 wherein the storing one or more cryptographic keys further comprises,

storing the one or more cryptographic keys in the off-line encryption device; and

storing the one or more cryptographic keys in the encryption renewal system.

23. The method of claim 19 further wherein the one or more cryptographic keys include any one or more of a secret shared key, a private key, and a public key.

24. The method of claim 17 wherein the clear content is audio or video content intended for a user.